Asia-Pacific
Economic Cooperation

Advancing Free Trade
for Asia-Pacific Prosperity

Building Randomness and Unpredictability into Aviation Security Countermeasure Development and Implementation

BEST PRACTICES GUIDELINES

APEC Transportation Working Group

February 2023

Asia-Pacific
Economic Cooperation

Building Randomness and Unpredictability into Aviation Security Countermeasure Development and Implementation

BEST PRACTICES GUIDELINES

APEC Transportation Working Group

February 2023

APEC Project: TPT 02 2020A

Produced by
U.S. Transportation Security Administration
6595 Springfield Center Drive, Springfield, VA 22150 USA
Tel: +1 571 227 1149
Email: Kalei.Hall@tsa.dhs.gov

For
Asia-Pacific Economic Cooperation (APEC) Secretariat
35 Heng Mui Keng Terrace Singapore 119616
Tel: (65) 68919 600 Fax: (65) 68919 690
Email: info@apec.org
Website: www.apec.org

© 2023 APEC Secretariat

APEC#223-TR-03.1

Table of Contents

Glossary

ACI	Airports Council International
APEC	Asia Pacific Economic Cooperation
AUI	Act of Unlawful Interference
AVSEC	Aviation Security
CCTV	Closed Circuit Television
CISA	U.S. Cybersecurity and Infrastructure Security
CTED	Counter-Terrorism Committee Executive Directorate
CTWG	APEC Counter-Terrorism Working Group
DGCA	Directorate General of Civil Aviation
DHS	U.S. Department of Homeland Security
EDD	Explosives Detection Dog
ETD	Explosives Trace Detection
FBI	U.S. Federal Bureau of Investigation
GCTF	Global Counterterrorism Forum
GTI	Global Terrorism Index
HHMD	Hand-Held Metal Detector
ICAO	International Civil Aviation Organization
ID	Identification
NCTC	U.S. National Counterterrorism Center
SARP	Standard and Recommend Practice
TAM	UNOCT Threat Assessment Models Programme
TPTWG	APEC Transportation Working Group
TSA	U.S. Transportation Security Administration
TWG	APEC Tourism Working Group
UK	United Kingdom
UN	United Nations
UNOCT	United Nations Office of Counter Terrorism
WTMD	Walk-Through Metal Detector

Executive Summary

Introduction and Approach

At the 2017 Asia Pacific Economic Cooperation (APEC) Transportation Ministerial Meeting, APEC reaffirmed its commitment to enhancing transportation security by:

- Improving Member Economies' capacity to mitigate vulnerabilities and counter terrorist threats;
- Engaging with other stakeholders within APEC (i.e., Counter-Terrorism Working Group (CTWG), Tourism Working Group (TWG)) and international organizations (i.e., International Civil Aviation Organization (ICAO));
- Encouraging participation in ICAO priorities, such as the development of Security Culture and human capability programs; and
- Minimizing security risks to transportation by encouraging economies to develop strong and informed security policies and to boost participation in security initiatives.

In light of APEC's commitments and in-line with priorities of international aviation organizations, the United States proposed and received APEC approval for Project TPT 02 2020A – *Building Randomness and Unpredictability into Aviation Security Countermeasure Development and Implementation*. The project was designed to enhance APEC Member Economies' risk mitigation capabilities by examining how to best leverage their existing resources to target specific threats and identify vulnerabilities, and to determine when, where, and how to allocate future resources. The project enabled Member Economies to develop and institute more sustainable aviation security (AVSEC) measures that will not only provide greater facilitation of passengers and goods in air transport, but also allow for sustained high levels of security across the operating system. Participants learned how to better leverage existing resources to mitigate the insider threat, thereby affording all Member Economies, regardless of their economic means, equal opportunity to develop and implement countermeasures considering their current resources, without major expenditure. Thus, creating a more secure, efficient, and sustainable transportation environment.

The objectives of the Project were four-fold:

1) Ensure participants understand the international standards and recommended practices (SARPs) for the application of random and unpredictable techniques in their AVSEC regime, with a focus on airport-level operations;
2) Increase participants' knowledge of the insider threat within the aviation domain, how to address security issues using risk-based approaches, and better leverage existing resources to mitigate that threat;
3) Build support for participants to implement randomness and unpredictability within their AVSEC operations through risk analysis principles and risk management to mitigate identified vulnerabilities; and
4) Foster evidence-based risk-informed decision making to support a more robust Security Culture.

This Best Practices Guidelines and the Project Summary, included at APEC Publication APEC#223-TR-01.1, reflect the achievement of these objectives.

1 Introduction

The United States, as Project Organizer through the U.S. Transportation Security Administration (TSA), and on behalf of the project co-sponsors Canada, New Zealand, Singapore, and Chinese Taipei, is pleased to present this Best Practices Guidelines as a project deliverable to assist Member Economies in building randomness and unpredictability into AVSEC policies and programs, and recalling best practices during the development and implementation process, in line with the 2020 Work Plan of the APEC Transportation Working Group (TPTWG).

This Best Practices Guidelines includes participant feedback, lessons learned, references and resources that were shared and agreed by the participants, speakers, and experts of the project.

1.1 Structure of the Document

This document is structured as follows:

- The **Executive Summary** introduces the project concept and its approach to building randomness and unpredictability into AVSEC policies and programs in APEC.
- **Section 1** outlines the project's objectives and methodology, and describes the intended deliverables.
- **Section 2** explores random and unpredictable policies and programs best practices from the Best Practices Guidelines, which is included in the Appendix.
- **The Appendix** complements the main document and outlines the Best Practices Guidelines.

1.2 Project Objectives

By introducing the concept of random and unpredictable AVSEC countermeasure implementation, this project addressed the risks associated with trusted insiders, complacency in the implementation of security controls and the negative impact this can have on their deterrent effect, and how to efficiently use limited resources to effectively target known threats and mitigate assessed risk. The application of random and unpredictable techniques is promoted in the ICAO SARPs of Annex 17 to the Chicago Convention, and provided for in the ICAO Security Manual (Doc 8973). As such, Member Economies are obligated to consider incorporating these techniques in their deployment of AVSEC resources in order to achieve effective security outcomes. Understanding and employing risk analyses and risk management principles allows for more targeted application and efficient use of resources to achieve the greatest security outcome, and promote the development of innovative approaches to AVSEC. Using these techniques and applying these principles ensure greater fiscal and resource management and support the sustainability of operations in light of the continued growth of the aviation sector and within an ever-changing threat environment. The implementation of random and unpredictable AVSEC countermeasures has sustained benefits for every economy, from economies that are in the early stages of developing their AVSEC programs to economies with established AVSEC programs, but it is particularly relevant for those operating with very limited AVSEC resources.

This project consisted of virtual workshop and webinar sessions, project evaluation instruments, such as questionnaires, follow-up surveys, and targeted interviews, and an Outreach Campaign Briefer, culminating in a Best Practices Guidelines to enhance Member Economies' security countermeasure policies and programs within the aviation domain. The workshops covered case studies of programs and best practices, how to create and tailor tactical responses to risk, the benefits of conducting risk analyses, identification of resources to leverage for risk mitigation, and an overview of the international SARPs that promote the implementation of countermeasures using random and unpredictable techniques.

The objectives of this project were four-fold:

1. Ensure participants understand the international SARPs governing the application of random and unpredictable techniques in their AVSEC regime, with a focus on airport-level operations.
2. Increase participants' knowledge of the insider threat within the aviation domain, how to address security issues using risk-based approaches, and better leverage existing resources to mitigate that threat.
3. Build support for participants to implement randomness and unpredictability within their AVSEC operations through risk analysis principles and risk management to mitigate identified vulnerabilities.
4. Foster evidence-based risk-informed decision making to support a more robust Security Culture.

1.3 Project Methodology

The target audience of this project were individuals directly involved in the development and/or operationalization of AVSEC measures and associated policies, programs, and regulations within APEC Member Economies, both at the domestic (regulator) level and airport (operator) level. It was imperative to have a good mix between regulator and operator level participants as the successful development and implementation of risk-based countermeasures require alignment of (and sometimes change in) the institutional mindset at both levels and throughout the aviation environment. Both need to work collaboratively to apply project principles and achieve project outcomes. Beneficiary profiles included Member Economy AVSEC officials, policy makers and regulators, as well as aviation industry stakeholders responsible for AVSEC.

Throughout the project, participants were required to complete and return pre- and post-workshop questionnaires by the end of the workshops and webinar, as well as participate in the follow-up survey and targeted interview; however, only a few participants were selected to participate in the latter activity. In these evaluation methods, each participant was encouraged to share their views and advice on the project's impact and efficiency as well as possible suggestions and policy implications for future APEC-related cooperation programs and activities.

All project activities, including workshops, were conducted in English.

1.4 Project Deliverables

As approved in the Project Proposal, the deliverables for the project were two-fold:

1. A Best Practices Guidelines (this document), which compiles the inputs from experts and participants collected during the workshops and project activities.
2. A Project Summary (refer to APEC Publication APEC#223-TR-01.1), which outlines the details of the project.

2 Random and Unpredictable Aviation Security Countermeasures Best Practices

Throughout the project, participants were encouraged to share best practices to build randomness and unpredictability into AVSEC countermeasure development and implementation within their respective economies through the project evaluation instruments and during the workshop itself. The initial set of recommendations were captured from inputs from the Part 1 Workshop and included in the Outreach Campaign Briefer that was shared with participants in March 2022. The Briefer may be found in APEC Publication APEC#223-TR-01.1. The Best Practices Guidelines, which may be found in the Appendix, expands on information already found in the Briefer and captures additional best practices and lessons learned over the course of the entire life of the project. The Guidelines provides key considerations participants noted throughout the project, as well as additional considerations where participants noted challenges in their own programs, namely where to start and how to develop or implement truly random and unpredictable AVSEC countermeasures. The Guidelines document is by no means an exhaustive list of best practices; however, it provides a true look at key principles explored in depth throughout the project and best practices, references and resources that participants and experts offered as crucial to building randomness and unpredictability into AVSEC countermeasure development and implementation.

Appendix – Best Practices Guidelines

Building Randomness and Unpredictability into Aviation Security Countermeasure Development and Implementation

(APEC Project No. TPT 02 2020A)

BEST PRACTICES GUIDELINES

REFERENCES and RESOURCES

This section provides valuable references and resources, many of which were provided by the project participants and experts, and which reinforce the best practices that can be found alongside the main section of this document. Additional Random and Unpredictable AVSEC Program resources are included at the end of the Best Practices Guidelines.

Fast Facts from Project TPT 02 2020A

- 86 individuals from 14 APEC Member Economies and several non-member industry organizations participated in the Project activities
- On average, 50% of participants had 1-5 years of AVSEC experience
- 62.2% of respondents to the pre-workshop questionnaire indicated their Economy employs random and unpredictable security measures within the aviation domain, including:
  - Explosives Trace Detection (ETD) (94.1%)
  - Behavior Detection (94.1%)
  - Secondary/Enhanced screening measures (88.2%)
  - Patrols (76.5%)
  - Identification (ID)/Credential checks (70.6%)
  - Monitored Closed Circuit Television (CCTV) (58.8%)
  - Explosives Detection Dog (EDD) (35.3%)
  - Other measures (23.5%)

OVERVIEW

From October 2020 to December 2022, the United States conducted Project TPT 02 2020A, entitled *Building Randomness and Unpredictability into Aviation Security Countermeasure Development and Implementation*, under the auspices of the Asia Pacific Economic Cooperation (APEC). Project activities included a Part 1: Virtual Workshop held 24 and 26 February 2021, a Mini Webinar held 4 August 2021, a Part 2: Virtual Workshop held 8-9 June 2022, a follow-up survey, targeted interviews, and pre- and post-workshop and webinar questionnaires. From the discussions and responses to the project evaluation instruments, key themes and best practices emerged and were captured in an Outreach Campaign Briefer, which was sent to participants midway through the project. This Best Practices Guidelines builds on those key themes and captures best practices from all project activities to assist economies with the development and implementation of random and unpredictable aviation security (AVSEC) policies and programs.

Assessing the Risk and Identifying Vulnerabilities

To determine appropriate countermeasures to implement within an airport, the appropriate authority, in collaboration with airport operators and stakeholders, should first **conduct a risk assessment**. The results of this assessment, when **considered along with intelligence from government and open sources**, should inform what and where resources should be applied and the specific countermeasures to be developed and implemented in order to more effectively mitigate the assessed risk. Risk is a function of vulnerability, threat, and consequence; when one factor changes, the others should also be reassessed to provide a current risk picture. Changes in the risk assessment may necessitate adjustments to previously developed countermeasures to ensure the mitigation measures that are implemented target the actual assessed risk and remain fit-for-purpose over time.

After conducting a risk assessment, the appropriate authority should identify any actual or potential vulnerabilities within its operations, considering the attack method and using root cause analysis to uncover the true cause of the vulnerability. This will aid in determining what measures are most effective to mitigate it. As mentioned above, vulnerability is not static and, therefore, **vulnerability identification requires on-going analysis using the information that is available at the time to inform decisions**. Compliance audits and tests may assist in identifying vulnerabilities, such as discovering gaps in security or lack of effective implementation of security requirements; however, compliance and vulnerability are not the same. Compliance is a rules-based program designed for mass application, typically across an economy and multiple operating environments. Whereas, **vulnerability identification is generally focused on local operations and in consideration of the threats to aviation security**; thus, vulnerability identification often occurs at the airport level or even the terminal or facility level to analyze threats specific to one airport and its operations. An aspect to

United Nations Office of Counter Terrorism (UNOCT)
http://un.org/counterterrorism

- The UNOCT Threat Assessment Models (TAM) Programme aims to consolidate multiple streams of expertise and assists economies to establish a common approach to threat assessments within the context of aviation security, build an interagency coordination model, and improve internal operational capacity to comply with international aviation security requirements

ICAO 40th Assembly SkyTalk: Aviation Security Risk Management
https://youtu.be/WDDIEUC1mlA

- Focuses on the ICAO aviation security risk assessment process, using methodologies found in ICAO Document 8973 and Document 10108, as well as its Risk Management Workshop

Airports Council International (ACI) Airports Risk Assessment Handbook
https://store.aci.aero/product/airport-security-risk-assessment-handbook-first-edition-2020/

- Assists airports with guidelines for understanding threats, assessing associated risks, and allocating resources where they are most needed

Assessing the Risk and Identifying Vulnerabilities (contd.)

consider when identifying vulnerabilities is: how much risk is associated with an identified vulnerability? Another question to consider is: when considering a specific identified vulnerability, **what is my economy or organization's risk appetite?**

Assessing vulnerabilities as high, medium, or low will allow one to rank their criticality to the security of the aviation system, and then prioritize which vulnerabilities should be first addressed and how resources should be allocated to do so. Generally, vulnerabilities are unlikely to be mitigated to zero, as there is always a measure of residual risk with everything; however, the aim of implementing appropriate mitigation measures is to 'buy down' risk, that is, to reduce a high criticality to medium, and a medium criticality to low.

Once vulnerabilities are identified and ranked, **root cause analysis should be used to determine the underlying reasons why the vulnerabilities exist and what can be done to correct them**. Asking the 'five whys' (asking why did something occur at least five times, or as many times as it takes until it is no longer possible to question why) will allow one to drill down to determine the causes of the vulnerabilities until the true root cause is uncovered. Typical root causes may be grouped into a few categories: human (operator error, human factors, social engineering); process or procedure (lack thereof, unclear); equipment (failure, malfunction, ineffective equipment for threat); or training (insufficient amount, ineffective). **Root cause analysis will not only assist in determining how to most effectively mitigate vulnerabilities, but also how, when, where, and what resources to allocate.** For example, implementing additional countermeasures to mitigate a vulnerability with a root cause of operator error (human) will not necessarily reduce the criticality of the vulnerability from high to medium. In most cases, remedial actions to address operator error (i.e., training, instruction, etc.) need to be taken before additional countermeasures are implemented. This will conserve budget, time, and energy while effectively addressing the underlying cause of the problem.

Determining the Appropriate Countermeasures

Considering the current threat picture and identified vulnerabilities, one can determine the most suitable and sustainable countermeasures to effectively mitigate the vulnerabilities. To begin, list the current security measures and capabilities in place at the airport, measures such as pat-down, hand-held metal detector (HHMD), walk-through metal detector (WTMD), body scanner, physical search of baggage, x-ray, explosives trace detection (ETD), explosive

The Global Terrorism Index (GTI)
https://www.visionofhumanity.org/maps/global-terrorism-index/#/

- Comprehensive study analyzing impact of terrorism globally

Examples of Random and Unpredictable AVSEC Countermeasures That May Also Be Used Outside the Security Checkpoint

- ID checks for passengers and non-passengers
- EDD patrols and searches
- Visible deterrence patrols with law enforcement
- ETD of targeted areas (e.g., hands, shoes, accessible property, etc.)
- Pat downs or HHMD
- Accessible property search
- Active monitoring of CCTV
- Behavior Detection
- Any of the above can also be mixed and matched with each other, as well as used in conjunction with a randomizer tool

Indonesia Directorate General of Civil Aviation Decree Number 221 Year 2020
https://www.dgca.gov.in/digigov-portal/

- Directorate General of Civil Aviation (DGCA) of Indonesia issued Decree 221 Year 2020 as a reference for all stakeholders at the airport to implement random and unpredictable AVSEC countermeasures

Determining the Appropriate Countermeasures (contd.)

detection dog (EDD), etc. **Then, add to this list any innovative and emerging technologies and measures and best practices from international organizations that may be available, and also discuss with partners globally or in the region what countermeasures have they employed to mitigate similar threats or vulnerabilities.** When developing countermeasures to specific vulnerabilities, the appropriate authority may start with the same preliminary list of AVSEC countermeasures that then should be customized to the specific vulnerabilities. For example, vulnerabilities that occur outside the standard security checkpoint should have countermeasures that are easily mobile, such as identification (ID) verification, pat-down, HHMD, physical search, some ETDs, EDD, etc. Static measures, such as WTMD, body scanner, or x-rays, should not be considered if the AVSEC countermeasure application location is far from where such equipment is located.

When customizing the AVSEC countermeasures list, consider what countermeasures are already in place that may address the threat. For example, if all passengers are screened by WTMD, conducting random and unpredictable HHMD search has a low countermeasure effectiveness because it does not add any additional effective layer of security, since both types of equipment detect only metallic threats. Additionally, **the AVSEC countermeasures implemented should be suitable to effectively mitigate the particular threat.** If the threat involves an on-body non-metallic explosive and the primary method of screening is WTMD, then the additional countermeasure should be one that is capable of detecting non-metallic threats on a person's body, such as a pat-down, body scanner, ETD, EDD, etc.

Multiple countermeasures may be effective at mitigating one vulnerability; therefore, consider as many countermeasures as possible that would be suitable to mitigate the vulnerability and that would be sustainable to implement. Conversely, a single countermeasure might be effective at mitigating multiple vulnerabilities. **Analyzing and applying a low, medium, or high rating of the effectiveness of each countermeasure vis-à-vis the identified vulnerability or threat will help to direct what and where resources should be allocated.** However, when creating an implementation plan, all effective countermeasures should be initially considered, not just those rated as highly effective. This will ensure all options are duly considered and the most effective (in terms of both security effectiveness and cost effectiveness) measures are applied.

Creating an Implementation Plan and Scheduling Random and Unpredictable AVSEC Countermeasures

Consider each suitable and sustainable effective countermeasure one-by-one, and then outline the frequency, personnel, equipment, and communication needs for each, as well as any additional relevant information regarding the location and operating environment where the

Civil Aviation Security in Mexico
https://www.gob.mx/afac/acciones-y-programas/seguridad-de-la-aviacion-civil

- Includes a list of procedures for the Prevention of Acts of Unlawful Interference (AUI)

"Soft Target Protection in an Aviation Ecosystem" APEC Workshop
https://www.state.gov/dipnote-u-s-department-of-state-official-blog/to-prevent-a-terrorist-attack-officials-are-working-to-improve-airport-security-worldwide/

- APEC Counter-Terrorism Working Group (CTWG) conducted a workshop that addressed terrorist attacks in airports, and refreshed the Global Counterterrorism Forum's (GCTF) Good Practices on the Protection of Soft Targets in a Counterterrorism Context

The Protection of Critical Infrastructure Against Terrorist Attacks: Compendium of Good Practices
https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/eng_compendium-cip-final-version-120618.pdf

- UNOCT and the United Nations (UN) Security Council Counter-Terrorism Committee Executive Directorate (CTED) created the Compendium as a tool to support stakeholders who have responsibilities for designing, improving, or implementing policies and measures to protect critical infrastructure against terrorist attacks

Creating an Implementation Plan and Scheduling Random and Unpredictable AVSEC Countermeasures (contd.)

different countermeasures will be implemented. **The risk assessment and intelligence should inform the frequency, along with the operational context**, but the schedule of implementation should still be random and unpredictable. With this information outlined, a daily, weekly, then monthly, and eventually yearly plan can be built, varying the countermeasures, hours of the day, and days of the week. **Each level (hour, day, week, month, year) should be different from the previous level so that no discernible pattern emerges as to when, where, and what countermeasure will be applied.**

While scheduling countermeasures that are supposed to be random and unpredictable may seem counterintuitive, **scheduling helps to ensure implementation is truly random and unpredictable for both those carrying out the measures and for the individuals who may be subjected to them.** To assist with scheduling in a random and unpredictable manner, many economies noted they use randomizer software. With this tool, economies can input possible countermeasures into the randomizer and it will generate a schedule to conduct said countermeasures at random and unpredictable intervals. While a randomizer tool may make generating schedules as easy as the push of a button, creating random and unpredictable schedules can be done manually just as effectively without additional resource expenditure. **Access to scheduling information and software should be safeguarded and treated as Sensitive Aviation Security Information**, so that only a limited number of authorized officials who are in charge of scheduling have access, and so that the information is not inadvertently or otherwise leaked in advance of implementation. Even the officers who are assigned to implement the countermeasures should not have access to their schedules until they are ready to be deployed. This will protect the randomness and unpredictability of the program as implemented and ensure individuals are not able to circumvent security.

Monitoring the Implementation of Random and Unpredictable AVSEC Countermeasures

Once the implementation plan and schedules have been created and the random and unpredictable countermeasures have been implemented, **the countermeasures should be reviewed periodically to ensure they are implemented appropriately and remain effective in mitigating the vulnerability, and to determine if adjustments to the schedule (frequency) should be made.** Adjustments may be needed periodically due to airport operations (e.g., seasonal surge or decline in operations, new construction or renovation works, etc.) or changes in the risk assessment and/or threat or as new intelligence becomes available.

Additionally, analyzing the data collected from these reviews, will assist in determining if the vulnerability criticality has been reduced because of these efforts. If the vulnerability criticality has not been reduced, a root cause analysis should be conducted to determine what aspect of the implementation plan is not fit-for-purpose or if there is some other cause that

Ishikawa Diagram
https://safetyculture.com/topics/ishikawa-diagram/

- An Ishikawa diagram, also called the Fishbone diagram, is often used to outline the different steps in a process, demonstrate where quality control issues might arise, and determine which resources are required at specific times

Building Local Targeted Violence and Terrorism Prevention Frameworks
https://www.dhs.gov/sites/default/files/2022-02/Building%20Local%20Prevention%20Frameworks_2.pdf

- This U.S. Department of Homeland Security (DHS) publication provides best practices for building effective local terrorism prevention frameworks through public awareness and education, threat assessment and management, and identification of stakeholders and resources

U.S. TSA Insider Threat Roadmap
https://www.tsa.gov/sites/default/files/3597_layout_insider_threat_roadmap_0424.pdf

- The TSA Insider Threat Roadmap defines the common vision for the U.S. Transportation Systems Sector that insider threat is a community-wide challenge, and outlines work with aviation stakeholders to refine and improve efforts to detect, deter, and mitigate insider threats, leveraging innovative concepts and technology

Monitoring the Implementation of Random and Unpredictable AVSEC Countermeasures (contd.)

may have been previously overlooked. For example, is the countermeasure not as effective as originally thought, does the frequency need to be increased, is the correct equipment being used, are the operators properly trained for these countermeasures, etc. If the vulnerability criticality has been reduced from high to medium, consider what more can be done to further reduce the criticality to low. If the vulnerability criticality has been successfully reduced to a low rating, celebrate your success but continue to monitor the program, current threat environment, and update the risk assessment to ensure the program and the applied countermeasures remain effective and relevant.

With on-going monitoring, further improvements can be made to the random and unpredictable AVSEC countermeasures program. Adversaries are adaptive; accordingly, AVSEC authorities must be flexible and agile to meet the ever-changing threat. **As technology and international best practices are improved, these should be incorporated into the random and unpredictable AVSEC countermeasures program, as appropriate.** If implementation plans only apply a defined suite of countermeasures, then an adversary can more easily determine which countermeasures they will need to circumvent, even if applied in a random and unpredictable manner. Therefore, countermeasure development and improvement should be conducted continuously to meet the current and evolving threat(s).

Coordinating with Stakeholders During the Development and Implementation Process

Where possible, coordinating with aviation stakeholders during key points when developing and implementing random and unpredictable AVSEC countermeasures can be very beneficial. **Stakeholders will have unique insights into the airport operations and additional threat and intelligence that should also be considered when assessing the risk and identifying vulnerabilities.** This is also true of non-aviation stakeholders, such as local law enforcement, other agencies operating in the airport (customs and border control) and intelligence organizations, who may have information to share with the appropriate authority on threats to transportation within the Economy.

Additionally, **stakeholder buy-in is key when implementing the countermeasures and to promote compliance with the new measures.** If a strong relationship is established with aviation stakeholders in advance, senior leadership from the aviation stakeholder organizations may be leveraged to communicate to their employees the new random and unpredictable AVSEC program for awareness and understanding. Such communication may convey that the measures will occur on a random and unpredictable basis and that all individuals are required to comply if subjected to them. Stakeholders may also be able to assist with the implementation of non-security screening aspects; for example, the airport

APEC Project TPT 07 2020A: *Building a Culture of Security and Countering the Insider Risk*
http://mddb.apec.org/Pages/search.aspx?setting=ListMeeting&DateRange=2022/03/01%2C2022/03/end&Name=Workshop%20on%20Building%20a%20Culture%20of%20Security%20and%20Countering%20the%20Insider%20Risk%202022

- Conducted from February 2021 to September 2022, TPT 07 2020A culminated in a Project Summary and Best Practices Guidelines that captured the key themes and best practices on building a culture of security from participating APEC Member Economies and industry organizations

ICAO Security Culture Self-Assessment Tool
https://www.icao.int/Security/Security-Culture/Pages/State-self-assessment.aspx

- Provides a series of questions that can assist to assess if an effective Security Culture exists and identify possible areas of improvement

United Kingdom (UK) Embedding Security Behaviour Change
https://www.cpni.gov.uk/embedding-security-behaviour-change

- Provides a cohesive approach to creating a coordinated strategy for security behavior change, including off-the-shelf campaigns and guidance documents

Coordinating with Stakeholders During the Development and Implementation Process (contd.)

operator may be able to close off some access doors to funnel employees to areas where the countermeasures will be implemented, thus increasing the encounter rate of the countermeasures.

Promoting Security Culture for Effective Security Countermeasure Implementation

Coordinating with aviation stakeholders is not only beneficial to the execution of the random and unpredictable AVSEC program, but it also assists to enhance the airport's Security Culture. **Security Culture plays an integral role in effective security countermeasure implementation, particularly when reinforced through strong leadership messaging, engagement and action.** It is vital for leadership at the highest levels to demonstrate and take actions that embody effective Security Culture. For example, if senior government and political leadership undergo security screening, to include random and unpredictable screening countermeasures, this visibly demonstrates to the public, airport employees, and security personnel the importance of security and its application at all levels.

Adding Random and Unpredictable Countermeasures to Baseline Security Measures

Understanding there is no one-size-fits-all approach, random and unpredictable AVSEC countermeasures should be implemented above, or in addition to, what the baseline security measures already provide. A random and unpredictable AVSEC program should be informed by a risk assessment, including local threat intelligence, and tailored to strengthen existing security measures at the airport. The application of random and unpredictable countermeasures is supplementary to the existing security requirements and processes already in place at an airport, providing an additional layer of security and targeting trusted insiders or others who try to 'game the system' or circumvent security. The benefit of a random and unpredictable AVSEC program is that it is adjustable, customizable, and scalable to any operating environment and risk context. It is a truly outcomes-focused program as analysis, development, implementation, and monitoring processes are undertaken to implement effective countermeasures in addition to the baseline measures to reduce the airport's vulnerabilities (outcome). In this regard, random and unpredictable AVSEC countermeasures are best applied as an "invisible" layer of security that allows the AVSEC operator to be innovative in its application of various methods, to include timing, location, equipment/technology, and procedure.

ADDITIONAL RANDOM AND UNPREDICTABLE PROGRAM AVSEC RESOURCES

- Part 1 Workshop Materials: http://mddb.apec.org/Pages/search.aspx?setting=ListMeetingGroup&DateRange=2021/02/01%2C2021/02/end&Name=Workshop%20on%20Building%20Randomness%20and%20Unpredictability%20into%20Aviation%20Security%20Countermeasure%20Development%20and%20Implementation%202021&APECGroup=%22Transportation%20Working%20Group%20%28TPTWG%29%22
- Mini Webinar Materials: http://mddb.apec.org/Pages/search.aspx?setting=ListMeeting&DateRange=2021/08/01%2C2021/08/end&Name=Webinar%20on%20Building%20Randomness%20and%20Unpredictability%20into%20Aviation%20Security%20Countermeasure%20Development%20and%20Implementation%202021
- Part 2 Workshop Materials: http://mddb.apec.org/Pages/search.aspx?setting=ListMeeting&DateRange=2022/06/01%2C2022/06/end&Name=Workshop%20on%20Building%20Randomness%20and%20Unpredictability%20into%20Aviation%20Security%20Countermeasure%20Development%20and%20Implementation%202022
- ICAO Security Culture Toolkit and Resources: https://www.icao.int/Security/Security-Culture/Pages/ICAO-Resources.aspx
- ICAO Year of Security Culture: https://www.icao.int/Security/Security-Culture/Pages/YOSC-2021.aspx
- ICAO Security Culture Webinar: https://www.icao.tv/videos/the-icao-security-culture-webinar
- ICAO Aviation Security Manual (Doc 8973): Random and Unpredictable Screening of a Proportion of Passengers (11.5.5); Unpredictability Principles and Measures (11.9); Threat and Risk Assessment Methodology (Appendix 37)
- Australian Government: A guide to developing and implementing a Suspicious Activity Identification Program at airports: https://www.icao.int/Security/Security-Culture/Documents/
- Sydney Airport: Security Awareness Guide: https://assets.ctfassets.net/v228i5y5k0x4/3NJHGSdSR3gM1giDE4a3iJ/141ae650cdefce75b37b557ed40be68d/Security_Awareness_Guide_V6.pdf
- Inside Look: TSA Layers of Security: https://www.tsa.gov/blog/2017/08/01/inside-look-tsa-layers-security
- ACI Asia-Pacific: Security Culture Explained Video: https://www.youtube.com/watch?v=STgTmVzzXyw
- IATA: Improving Performance through Security Culture: https://www.icao.int/Security/Security-Culture/Articles/An%20Article%20by%20IATA.pdf
- U.S. Cybersecurity and Infrastructure Security (CISA): Insider Threat Mitigation Guide: https://www.cisa.gov/sites/default/files/publications/Insider%20Threat%20Mitigation%20Guide_Final_508.pdf
- U.S. Federal Bureau of Investigation (FBI): The Insider Threat: An Introduction to Detecting and Deterring an Insider Spy: https://www.fbi.gov/file-repository/insider_threat_brochure.pdf/view
- U.S. National Counterterrorism Center (NCTC): Reporting Suspicious Activity – Critical for Terrorism Prevention: https://www.dni.gov/files/NCTC/documents/jcat/firstresponderstoolbox/133s_-_First_Responders_Toolbox_-_Reporting_Suspicious_Activity__Critical_for_Terrorism_Prevention.pdf
- UK Center for Protection of National Infrastructure: Security Culture Materials: https://www.cpni.gov.uk/

CONTACT US

Do you have additional best practices and/or resources to include? Please send your ideas and advice to Kalei.Hall@tsa.dhs.gov.